Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 03 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- Reuters reports the potential for power failures in the Midwest, due to high energy demand and rough weather, poses the biggest threat to the region's fuel production this summer. (See item 3)
- United Press International reports that the U.S. and Saudi governments said Wednesday that five more branches of al−Haramain Islamic Foundation were involved in financing terrorist groups. (See item 7)
- CNN reports that France has gone on red security alert for the visit of a host of world leaders at the weekend for the 60th anniversary of the D−Day landings. (See item 35)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 02, Reuters* — **UAE to pump more oil. The United Arab Emirates (UAE), the only member of the Organization of Petroleum Exporting Countries (OPEC) along with Saudi Arabia with any significant spare capacity, will lift crude output in June by 400,000 barrels per day,** Oil Minister Obaid al−Nasseri said on Wednesday, June 2. He added that the OPEC producers' group should raise its output ceiling by more than two million bpd to help cool scorching prices, which have hit a new 21−year high at $42.45 a barrel for U.S. crude. Ministers from OPEC are due to meet in Beirut, Lebanon, on Thursday, June 3, to review

production policy.
Source: http://www.nytimes.com/reuters/business/business−energy−uae− opec.html

2. *June 02, Associated Press* — **Storms black out a half−million in Texas.** Thunderstorms Tuesday, June 1, pounded parts of Texas with hail as big as tennis balls and wind blasting to more than 80 mph, halting flights at two airports and blacking out more than a half−million customers. By Wednesday, June 2, the storms had blown east into Louisiana and Mississippi, but more storms were possible in Texas late Wednesday. **More than a half−million customers lost power at the height of the storms, said TXU Electric Delivery spokesperson Scott Withers. He said power was restored to about 170,000 customers before daybreak, but it could be days before all service is back to normal.** Elsewhere, a new swarm of storms packing wind of up to 70 mph hit West Virginia on Tuesday, killing a truck driver, knocking down trees and power lines and blacking out 103,000 utility customers. Power outages in western West Virginia could last into the weekend, said utility provider AEP spokesperson Phil Moye.
Source: http://abcnews.go.com/wire/US/ap20040602_551.html

3. *June 02, Reuters* — **MAP says power grid biggest threat to refineries.** The potential for power failures in the Midwest due to high energy demand and rough weather poses the biggest threat to the region's fuel production this summer, the head of Marathon Ashland Petroleum LLC (MAP) said on Wednesday, June 2. "The biggest concern for refinery operations is the power grid. Coming into summertime and with the violent storms we have seen, it is clear to us the power grid is stretched," said MAP President Gary Heminger. MAP runs seven U.S. refineries with a combined crude distillation capacity of roughly one million barrels per day (bpd). **The bulk of MAP's operations are in the Midwest, a region that has been strafed by deadly storms over the past couple of weeks and which is particularly sensitive to refinery problems due to a shortfall in the region's fuel production capacity. Oil refinery operations can be brought to a swift and sometimes damaging halt during a power grid failure.**
Source: http://biz.yahoo.com/rc/040602/energy_map_refineries_1.html

4. *June 02, Star−Telegram (TX)* — **No cause found yet in outage at nuclear plant.** A cause has not been determined for an hourlong complete power outage at a nuclear weapons plant near Amarillo, TX, and the investigation is expanding, an official said Tuesday, June 1. The May 19 blackout affected the entire Pantex plant, America's only nuclear weapons assembly and disassembly facility, but backup power kicked in "very, very quick," said Jud Simmons, plant spokesperson. **Simmons said that it was the most severe power outage ever at the plant −− a depository of large amounts of radioactive materials −− but that security was never compromised.** After more than two weeks of searching for a cause for the outage, Simmons said the internal probe has expanded, including hiring additional people to investigate. In the May 19 power outage at Pantex, Simmons would not comment on whether officials had ruled out sabotage of the power system.
Source: http://www.dfw.com/mld/dfw/news/state/8817333.htm?1c

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *June 02, Reuters* — **Army issues order to stop U.S. soldiers from leaving. The U.S. Army has issued an order preventing thousands of soldiers designated for duty in Iraq or Afghanistan from leaving the military even when their volunteer service commitment expires,** officials said on Wednesday, June 2. The move to extend the service of some soldiers involuntarily was the latest sign of increasing stress on the Army as the Pentagon strives to maintain adequate troop levels in the two conflicts. **Lt. General Franklin Hagenbeck, the Army's personnel chief, denied that the move was a sign of desperation for the Army, although he did acknowledge that the Army was "stretched."** The "stop loss" order means that soldiers, who otherwise could leave the service when their volunteer commitments expire, starting 90 days before being sent, will be compelled to remain to the end of their overseas deployment and up to another 90 days after they come home. A "stop movement" order blocks soldiers from shifting to new assignments during the restricted period. Army spokespersons were unable to give a figure for how many soldiers would be affected by the orders beyond saying it will be in the thousands.
   Source: http://abcnews.go.com/wire/US/reuters20040602_171.html

6. *May 03, General Accounting Office* — **GAO−04−554: Joint Strike Fighter Acquisition: Observations on the Supplier Base (Report).** As the Department of Defense's (DoD) most expensive aircraft program, and its largest international program, the Joint Strike Fighter (JSF) has the potential to significantly affect the worldwide defense industrial base. As currently planned, it will cost an estimated $245 billion for DoD to develop and procure about 2,400 JSF aircraft and related support equipment by 2027. In addition, the program expects international sales of 2,000 to 3,500 aircraft. **If the JSF comes to dominate the market for tactical aircraft as DoD expects, companies that are not part of the program could see their tactical aircraft business decline. Although full rate production of the JSF is not projected to start until 2013, contracts awarded at this point in the program will provide the basis for future awards.** General Accounting Office (GAO) was asked to determine the limits on and extent of foreign involvement in the JSF supplier base. Highlights:
   http://www.gao.gov/highlights/d04554high.pdf
   Source: http://www.gao.gov/new.items/d04554.pdf

[Return to top]

Banking and Finance Sector

7. *June 02, United Press International* — **U.S., Saudi name terror financiers. The U.S. and Saudi governments Wednesday, June 2, said five more branches of al−Haramain Islamic Foundation were involved in financing terrorist groups.** The two countries are submitting the entities to the United Nations to be added to the list of terrorists tied to al Qaeda, Osama bin Laden and the Taliban, the statement said. Aqeel Abdulaziz Al−Aqil, the former leader of the

group, has also been designated, the statement said. Inclusion on the UN list requires member states to freeze the assets of the groups. The Department of Treasury is designating al−Aqil and the branches of AHF in Afghanistan, Albania, Bangladesh, Ethiopia and the Netherlands to its list of terrorist financiers.
Source: http://www.washingtontimes.com/upi−breaking/20040602−120237− 5292r.htm

8. *June 02, Newsday (NY)* — **Identity theft case nets terror link.** An identity theft case in Farmingville, NY, led Suffolk, NY, police to a couple with possible ties to terrorism operating a virtual credit card factory out of their Brooklyn, NY, apartment, Suffolk prosecutors said. **Police found more than 1,000 credit card numbers, blank and cloned credit cards, credit card readers and encoders, and various computer equipment during an early morning raid** on Thursday, May 27. Yunus Unlu, a Turkey national, and Sai Jiang, a Chinese citizen, are being held without bail in the Suffolk County jail in Riverhead pending their arraignment. Also seized in the apartment were various passports, New York State driver's licenses and Social Security cards in their names. Police found more than $17,000 in cash, but it is still unknown exactly how much money is involved or how many victims. **Detectives with the Identity Theft Unit believe the couple were funding terrorist activities.** Police said they are still unsure if they know the exact identities of the suspects, as they have various aliases.
Source: http://www.newsday.com/news/local/longisland/ny−itheft0603,0 ,2763040.story?coll=ny−topstories−headlines

9. *June 02, Netcraft* — **Phishing worm installs trojan without trickery.** The threat posed by phishing has racheted up a notch with the Korgo worm, which auto−infects unpatched Windows systems with a keylogging trojan, steals online banking information, and secretly transmits data back to the fraudsters. **The worm represents an alarming advance in phishing, as it forgoes the need to trick the end user into divulging details. Korgo uses the LSASS vulnerability to auto−infect Windows systems that haven't applied the MS04−11 patch issued April 11.** Korgo's phishing activities were documented by F−Secure, a cyber security firm, which reports that the associated trojan is aggressively stealing user information from infected machines. "It does this via a keylogger which specifically collects user logins for online banks (the ones which do not use one−time passwords)," writes F−Secure's Mikko Hypponen. "It also logs everything the user types to any web form −− this will collect lots of credit card numbers, passwords etc." That information is sent to one of 11 geographically distributed Internet Relay Chat (IRC) servers, including eight different servers on the Undernet IRC network, which claims to have 45 servers in 35 countries.
Source: http://news.netcraft.com/archives/2004/06/02/phishing_worm_i nstalls_trojan_without_trickery.html

10. *June 01, Internal Revenue Service* — **IRS warns of scheme to steal identity and financial data. The Internal Revenue Service (IRS) warned on Tuesday, June 1, of a fraudulent scheme targeting non−resident aliens who have income from a United States source.** The scheme uses fictitious IRS correspondence and an altered IRS form in an attempt to trick the foreign persons into disclosing their personal and financial data. The information fraudulently obtained is then used to steal the taxpayer's identity and financial assets. **This scheme has surfaced in South America, Europe and the Caribbean so far.** In this particular scam, an altered IRS Form W−8BEN, "Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding," is sent with correspondence purportedly from the IRS to non−resident

aliens who have invested in U.S. property, such as securities or bonds, and therefore have U.S.−sourced income. The correspondence's threat is baseless. Genuine Forms W−8BEN are sent to the recipients by their financial institution, not by the IRS. The W−8BEN is used by the financial institution to establish the appropriate tax withholding or to determine whether their customers meet the criteria for remaining exempt from tax reporting requirements.
Source: http://www.irs.gov/newsroom/article/0,,id=123621,00.html

[Return to top]

Transportation Sector

11. *June 02, Associated Press* — **Two American Airlines planes receive bomb threats. Airliners about to take off from Philadelphia and Boston were searched Wednesday, June 2, after authorities received a telephoned bomb threat against the two American Airlines flights,** authorities said. Philadelphia International Airport officials evacuated 19 passengers from American Airlines Flight 4543 at about 6:30 a.m., airport spokesman Mark Pesce said. Pesce said the passengers were rescreened while the plane was searched. Nothing was found, he said. The flight to Boston was canceled anyway, the airline said. Later, in Boston, a connecting flight to London's Heathrow Airport, American Airlines Flight 156, was searched at Logan International Airport as it was about to take off. Nothing was found and the flight was allowed to take off with 159 passengers, American Airlines spokesperson Jacquie Young said. **Young said a telephone bomb threat received in Philadelphia mentioned both American flights.** Philadelphia police said the call was placed to the Embassy Suites Hotel Philadelphia−Airport, whose staff reported it to authorities. **The FBI and state law enforcement officials are investigating.**
Source: http://www.usatoday.com/travel/news/2004−06−02−plane−threat_x.htm

12. *June 02, Associated Press* — **Downeaster to shut down during DNC. Operators of Amtrak's Downeaster announced Wednesday, June 2, that they will suspend service between Portland and Boston during the week of next month's Democratic National Convention.** Security measures imposed on the rail line during the convention from July 26 to 29 were burdensome, said John Englert, executive director of the Northern New England Passenger Rail Authority. Workers will use the time to make rail improvements as the Downeaster prepares for a speed increase this summer. On August 1, the Downeaster's speed will be boosted along much of the track owned by Guilford Rail System, shaving five to 10 minutes off the trip between Portland and Boston, Englert said. The top speed will be 79 mph along four miles of the Guilford−owned track.
Source: http://www.thebostonchannel.com/news/3373744/detail.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *June 02, Reuters* — **EU set to debate two new GM approvals. European Union (EU) ministers and experts will this month consider two approvals for gene−spliced foods, just a few weeks after the bloc lifted a five−year biotech ban, officials said on Wednesday, June 2.** If authorized, the two products −− both marketed by U.S. biotech company Monsanto −− would be used in animal feed and industrial processing, not for growing in Europe's fields. The first vote should be taken on June 16 by environment experts representing the EU's 25 member states for a rapeseed known as GT73, modified to resist the non−selective herbicide glyphosate to allow farmers to manage weeds more effectively. Politically, the precedent now exists for more genetcally modified (GM) organism approvals after the European Commission lifted the bloc's effective moratorium on allowing new GM products. Later in June, EU environment ministers will discuss a possible second GM approval at a meeting scheduled for June 28. This GM product is a biotech maize called NK603, also modified to resist the glyphosate herbicide.
Source: http://www.forbes.com/markets/commodities/newswire/2004/06/0 2/rtr1391974.html

14. *June 02, Kansas Ag Connection* — **Unidentified virus appears in Kansas wheat fields. The pathogen causes wheat leaves to yellow and die, but it's not caused by wheat streak mosaic, head death, or freeze.** "We're pretty sure it's a virus," said wheat breeder Joe Martin, who works at the Kansas State University research station at Hays. "It showed up early and, at first glance, we thought it was streak mosaic. But it's not. It kills the oldest leaves of the plant and finally kills the head." **Researchers don't know what the virus is, where it came from, or how it spreads. Martin said he's seen evidence of the virus in almost every field he's checked in western Kansas, but it hasn't taken over the crop.** Dallas Seifers, a plant pathology professor at Fort Hays State University, is trying to determine how the pathogen works, and what it might be. "It's possible that this is something that has been identified somewhere else in the world, even something that has shown up in a different crop, corn or rice or something," Seifers said. Seifers, with the help of some virologists in Winnipeg, Canada, is trying to identify the protein that causes the virus' symptoms. That's complicated by the fact that most affected plants found in the field are already dead. Seifers is trying to grow his own supply of infected plants to study, but the effort hasn't been as successful as he hoped.
Source: http://www.kansasagconnection.com/story−state.cfm?Id=274&yr= 2004

[Return to top]

Food Sector

15. *June 02, Oster Dow Jones Commodity News* — **Meat industry's food safety investments.** The U.S. Department of Agriculture's (USDA) Economic Research Service (ERS) has released a new report on food safety investments made by meat and poultry processors during the years 1996 through 2000. The report, titled "Meat and Poultry Plants' Food Safety Investments: Survey Findings, May 2004," is based on a national survey of meat and poultry slaughter and processing plants about the types and amounts of food safety investments that were made during the five year period from 1996 to 2000. **An ERS release said the "report provides evidence that the industry has invested significantly in more sophisticated food safety**

technologies and those expenditures have had a direct impact on the safety of the food supply and practices that control or reduce pathogens." The survey found that during the five−year period, U.S. plants as a group spent about $380 million annually and made $570 million in long−term investments to comply with USDA's 1996 Hazard Analysis and Critical Control Point (HACCP) regulation. The USDA also said that during the same five−year period, the U.S. meat and poultry industry spent an additional $360 million on food safety investments that were unrelated to the HACCP rule. The report is available at: http://www.ers.usda.gov/publications/tb1911/tb1911_researchb rief.pdf.
Source: http://www.agprofessional.com/show_story.php?id=25428

16. *June 02, Agence France Presse* — **Philippines orders baby food recall over poison threat. Regulators said they had ordered a recall of certain Gerber baby food products in the Philippines after the local distributor received a threat that a shipment had been laced with poison. The sender of the threatening e−mail warned that 25 bottles of Gerber products had been laced with arsenic,** said Joyce Sirunay, regional division chief of the government's Bureau of Food and Drugs. The local distributor had been ordered to recall products specifically mentioned in the threat, she said over DZMM radio. Gerber Philippines took out newspaper advertisements Wednesday, June 2, to announce the recall, while insisting that no evidence of tampering had been found. Spokesperson for Gerber Philippines said the recall was ordered due to "information given to us" on Tuesday, June 1, about product tampering, but would not provide details. The police and the National Bureau of Investigation are looking into the case, they company added.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=15 07&e=6&u=/afp/20040602/hl_afp/philippines_food_health_040602 171054

17. *June 01, Associated Press* — **Expanded testing for mad cow begins. The U.S. Department of Agriculture (USDA) began expanded national testing for mad cow disease Tuesday, June 1, intending to test about 220,000 animals for the brain−wasting condition over the next year to 18 months.** Officials said the USDA was able to handle the first day's samples even though most of the dozen regional laboratories aren't yet equipped to perform the initial tests. The government last year conducted mad cow tests on tissues from 20,543 animals. After the nation's first case of the disease in December 2003, the USDA initially doubled the number of animals to be tested this year to 40,000. With many foreign governments still reluctant to ease bans on U.S. beef, the testing program was expanded at a cost of $70 million to include as many as 220,000.
Source: http://www.mlive.com/newsflash/business/index.ssf?/newsflash /get_story.ssf?/cgi−free/getstory_ssf.cgi?f0338_BC_MadCow&&n ews&newsflash−financial

18. *June 01, Food and Drug Administration* — **Royal Candy recalls nuts. Royal Candy &. Nut Co. is conducting a voluntary recall on its distribution of raw whole almonds and California mix packaged as Royal Candy products due to the possibility of contamination with Salmonella enteritidis.** Salmonella is an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Royal Candy & Nut, Co. distributes this product in Illinois and Indiana. This recall is in follow up to a voluntary recall announced in mid−May by Paramount Farms of California of whole and diced raw almonds based on over 20 possible cases of illnesses associated with the almonds.

Source: http://www.fda.gov/oc/po/firmrecalls/royal05_04.html

19. *June 01, Pro Farmer* — **Indonesia resumes imports of U.S. beef. Indonesia has lifted its ban on imports of U.S. beef, becoming one of the first countries besides Mexico and Canada to resume their imports of U.S. beef since such shipments were halted by many countries after the U.S. announced it found its first case of mad cow disease on December 23, 2003.** U.S. beef accounted for only four percent of Indonesia's imports, as they take most of their supplies from Australia and New Zealand. However, this is still being taken as a positive sign since Indonesia cited a determination last week by the OIE (international animal health organization) that the U.S. was now considered to be BSE free. This may prompt other countries to follow up and resume their imports of U.S. beef. Japan, the largest buyer of U.S. beef, still has a ban in place and talks between the two sides are ongoing.
Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsArticle_200461849_136&articleid=108884&newscat=GN

[Return to top]

Water Sector

20. *June 01, Florida Today* — **Drier weather drains water supply. Without rain, water officials say, Melbourne, FL, could be in for harsher watering restrictions.** Homeowners consumed 20 percent to 40 percent more water last month as they tried to save their lawns from wilting in May's dry weather, drawing the water supply to near−critical levels, water officials said. Water providers want people to voluntarily cut back on watering until hoped−for June rains replenish lakes and wells. May is traditionally a high irrigation month, said Al Canepa, assistant director of the department of resource management for the St. Johns Water Management District. **Groundwater has dropped a foot and a half since last year, Canepa said, from 39 feet above mean sea level to 37.5 feet. The monthly average since the 1930s is 40 feet.** It's nowhere near the all−time record low, Canepa said. "It's getting to an area where if we don't start to get rainfall, then we'll start to become concerned," he said. Brevard County is currently under a water restriction order imposed by the St. Johns Water Management District in 1991 that prohibits watering between 10 a.m. and 4 p.m. Cocoa and Titusville water customers are on a 2001 order that also limits watering to two days a week. Palm Bay is under the same restrictions as Melbourne.
Source: http://www.floridatoday.com/!NEWSROOM/localstoryN0602WATERUS E.htm

21. *June 01, Philadelpia Business Journal* — **Aqua America acquires Heater Utilities. Aqua America Inc. said Tuesday, June 1, it has completed an acquisition that makes it the largest nonmunicipal water and wastewater utility in North Carolina.** In the deal, Aqua America, which is based in Bryn Mawr, PA, acquired Heater Utilities Inc., which is based in Cary, NC. The seller was Allete Water Services Inc., a subsidiary of Allete Inc., a conglomerate based in Duluth, MN. **Aqua America, which is the largest publicly traded water utility based in the United States, paid $76 million for Heater Utilities.** The acquisition will give Aqua America more than 48,000 additional water customers and 6,000 additional wastewater customers, bringing the total number of customers it serves in North Carolina to more than 175,000.
Source: http://philadelphia.bizjournals.com/philadelphia/stories/200 4/05/31/daily7.html

[Return to top]

Public Health Sector

22. *June 02, Ravalli Republic (MT)* — **Scientist infected with Salmonella. A Rocky Mountain Laboratories (RML) microbiologist who conducts research on Salmonella got sick from the bacteria in the lab.** The scientist came down with food poisoning, a common food−borne infection caused by Salmonella in late April, and officials at the Montana Public Health Laboratory confirmed Friday, May 28, that the infection was acquired in the Hamilton lab. An experienced scientist at RML, the worker sought treatment from a local physician and was admitted to a hospital, RML Associate Director Marshall Bloom said. The state lab did three independent tests to confirm that the Salmonella strain that infected the lab worker was the same used in research at RML, a biological research facility under the National Institute of Allergy and Infectious Diseases. Salmonella is generally contracted through the mouth, but it is uncertain just how the scientist got the disease. No other lab employees or family members are known to have developed symptoms of salmonella as a result to exposure to the employee who was ill.
Source: http://www.ravallinews.com/articles/2004/06/02/news/news01.t xt

23. *June 02, CBC (Canada)* — **China says SARS outbreak over.** China says the latest outbreak of Severe Acute Respiratory Syndrome (SARS) has been brought under control. **Authorities closed the SARS prevention headquarters in Beijing and the health ministry stopped its daily surveillance reports on the disease on Tuesday, June 1.** China had reported nine SARS cases in April and May, seven in Beijing and two in the eastern province of Anhui. One person died. All the cases have been linked to the National Institute of Virology in Beijing, which carried out experiments using SARS. **The decision to declare the outbreak over was made after seven patients recovered and were released, the official Xinhua news agency reported.** People under observation for having had contact with suspected cases of SARS were released from isolation.
Source: http://www.cbc.ca/stories/2004/06/02/world/sars040602

[Return to top]

Government Sector

24. *June 02, Department of Homeland Security* — **Department of Homeland Security announces award of US−VISIT contract.** Asa Hutchinson, Under Secretary of Border and Transportation Security for the Department of Homeland Security announced the selection of a prime contractor for US−VISIT to help strengthen security at America's borders and modernize the border management process Wednesday, June 2. The contract covers a base period of five years, with five one−year options. The contract value is for a minimum of $10 million and a maximum of $10 billion. The prime contractor will provide a wide range of professional services including strategic support, design and integration activities, technical solutions, deployment activities, training, and organizational change management. **Currently, US−VISIT requires that most foreign visitors traveling to the United States on a visa and arriving at**

an air or seaport have their two index fingers scanned and a digital photograph taken to verify their identity at the port of entry. By September 30, 2004, this process will also apply to visitors traveling under the visa waiver program at all air and sea ports of entry. Source: http://www.dhs.gov/dhspublic/display?content=3694

[Return to top]

Emergency Services Sector

25. *June 02, Associated Press* — **Feds: Air tankers my be used this summer. Some large air tankers that had been grounded over safety concerns could be back fighting fires this summer if their private operators can prove they are safe to fly, federal officials said Wednesday, June 2. The Forest Service grounded the 33−plane fleet last month because it had no way to tell if the aging planes were safe. But officials said Wednesday they have worked with the Federal Aviation Administration to develop guidelines to assess the planes' air worthiness.** The private companies that operate the military surplus planes will be asked to supply detailed records showing each plane's flight history, maintenance and other information, said Mark Rey, the Agriculture undersecretary who oversees the Forest Service. Once that information is received, the Forest Service will work with the FAA and the National Transportation Safety Board to determine what planes can be returned to service, Rey told the Senate Commerce Committee. Pressed by lawmakers as to when the planes could be back in use, Rey said some will probably never return. But others could be returned to service in about 30 days, he said. News of the possible return of some air tankers followed an announcement Tuesday, June 1, that the Forest Service and Bureau of Land Management will contract for nearly 130 more aircraft to fight wildfires this summer.
Source: http://www.wtopnews.com/index.php?nid=116&sid=209433

26. *June 01, Government Technology* — **Kansas City upgrades fire and police public safety systems.** The Kansas City Fire Department has successfully completed the installation of a new computer aided dispatch (CAD) and records management system (RMS). The system is the first phase of an $8.6 million contract to provide new public safety systems for the city's police and fire departments. The new CAD system replaces an outdated system, and will allow dispatchers to respond to and manage citizen's requests for fire and rescue services more efficiently. "Installing a reliable system is critical to any public safety operation," said Rick Brisbin, project manager for Kansas City. "We have not experienced any downtime since we took the system live." **A comprehensive mapping component provides dispatchers the ability to quickly assess the location of an incident and provide responding firefighters directions or details of the building, if required. With a couple of keystrokes, the new CAD system automatically pinpoints a caller's location, recommends appropriate apparatus to respond, alerts the fire stations and tracks the details of the fire response.**
Source: http://www.govtech.net/news/news.php?id=90453

[Return to top]

Information Technology and Telecommunications Sector

27. *June 02, ZDNet (UK)* — **Security contractors urged to take out personal indemnity insurance.** The increasing number of virus and worm attacks means that significant numbers of security contractors could face legal action after their client's systems have been attacked, say industry experts There was more virus and worm activity in the first three months of 2004 than in the whole of last year, and despite efforts by software and hardware vendors to address the problems, the situation seems to be getting worse. **As the number of attacks increases, there is an increasing risk that consultants will be blamed for disrupted services and lost data.** Stuart Okin, Microsoft UK's chief security officer, said he's not surprised that security professionals are having to take out indemnity insurance, but he believes that taking legal action against contractors is the wrong option. Instead, he said more resources should be ploughed into catching malware writers who are actively seeking out and exploiting security vulnerabilities.
Source: http://news.zdnet.co.uk/internet/0,39020369,39156428,00.htm

28. *June 02, The Register* — **Attack of the bandwidth−hogging hackers.** Swiss security researchers from the Ecole Polytechnique Federale de Lussanne (EPFL)have unearthed a flaw in wireless LAN systems that might be used by hackers to drastically increase their share of the available bandwidth at the expense of the other users. **Appropriate standards (such as 802.11i) have been developed to ensure user security and privacy in hotspots, but this does nothing to prevent users altering the MAC protocol of a machine to increase his share of available**, according to the team. Professor Jean−Pierre Hubaux, leader of the team, said that although they had demonstrated these attacks in a lab environment they were yet to see reports about this kind of misdeeds in the real world yet. But that is no reason for complacency, he argued. "Experience has shown that breaches are usually exploited, especially if this is easy to do (as it is the case here). With the increasing programmability of the devices, the risk will increase as well," he said. EPFL researchers will present their work at the Mobisys mobile system conference in Boston next week.
Source: http://www.theregister.co.uk/2004/06/02/bandwidth_hogging_ha ckers/

29. *June 02, The Christian Science Monitor* — **Via eavesdropping, terror suspects nabbed.** An ordinary−looking grid map of Riyadh adorns one wall of a command−and−control center deep inside a government building in Saudi Arabia's capital. The map is higher−tech than it appears at first glance. Tiny embedded lights flash red when certain cellphones−−those belonging to suspected terrorists−−initiate or receive a call. Teams of officials from Saudi Arabia, the FBI, the CIA, and the U.S. Treasury Department decide instantly whether simply to watch and listen to the suspected terrorist−−or to send in police to nab him. Subscriber Identity Model (SIM) cards, were developed to create a universal−−and cheaper−−cellphone system. SIM cards contain a fingernail−sized computer chip. Information on pricing, minutes, and local telephone numbers is encoded in the chip. Since there is no need for a local record of the purchaser's name and credit information, as there is when setting up a land line or a traditional cellphone account, it is easier for people to use phones undetected. **After years of tracking terrorists, investigators have amassed a large database of land−line and traditional cellphone numbers they are monitoring. All it takes is a call from one of those numbers to a phone with a SIM card to discover who's using the undetectable phone.**
Source: http://www.csmonitor.com/2004/0602/p02s01−usmi.html

30. *June 02, General Accouting Office* — **GAO−04−706: Information Security: Continued Actions Needed to Improve Federal Software Patch Management (Report).** Flaws in

software code can introduce vulnerabilities that may be exploited to cause significant damage to federal information systems. Such risks continue to grow with the increasing speed, sophistication, and volume of reported attacks, as well as the decreasing period of the time from vulnerability announcement to attempted exploits. The process of applying software patches to fix flaws, referred to as patch management, is a critical process to help secure systems from attacks. The Chairmen of the House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census requested that GAO assess the (1) reported status of 24 selected agencies in performing effective patch management practices, (2) patch management tools and services available to federal agencies, (3) challenges to performing patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities. **GAO recommends that the Director of OMB issue guidance to agencies to provide more refined information on patch management practices, and determine the feasibility of providing selected centralized patch management services**. Highlights: http://www.gao.gov/highlights/d04706high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−706

31. *June 01, Federal Computer Week* — **Cooperation, wireless, top NASCIO agenda.** Wireless communications interoperability and intergovernmental cooperation are among the top issues that state chief information officers plan to discuss with members of Congress in Washington, DC this week. CIOs from 15 states are participating in the National Association of State CIOs' fourth annual fly−in. They have a number of state information technology issues that they plan to bring up, including the lack of state cybersecurity planning in the Department of Homeland Security's preparedness plans; the need for federal agencies to help and support state enterprise architecture efforts through funding and coordination of standards and methodologies; the removal of barriers to multiagency and multigovernment programs put in place because of federal funding requirements; and the impact on state budgets and plans from federal privacy requirements. The meetings will culminate June 3 with a half−day roundtable among federal, state and local IT officials. This year, **the roundtable will focus on the role of state CIOs in achieving wireless interoperability**, which is one of the top issues across all levels of government, particularly in the law enforcement and homeland security arenas.
Source: http://fcw.com/geb/articles/2004/0531/web−nascio−06−01−04.as p

32. *May 28, Government Accounting Office* — **GAO−04−666: Spectrum Management: Better Knowledge Needed to Take Advantage of Technologies That May Improve Spectrum Efficiency (Report).** Recent advances in technologies such as cellular telephones, wireless computer networks, and global positioning system receivers that rely on the use of the radiofrequency spectrum have become critical to a variety of government missions, including homeland security and strategic warfare. However, **with the increased demand, the radio−frequency spectrum—a resource that once seemed unlimited—has become crowded and, in the future, may no longer be able to accommodate all users' needs**. As a result, there has been a growing debate among spectrum policy leaders about how to use spectrum more efficiently. GAO was asked to look at agencies' investments in spectrum efficient technologies and how the nation's spectrum management system may affect the development and adoption of these technologies. **GAO is making six recommendations intended to facilitate greater investment by federal agencies in spectrum efficient technologies. Overall, the agencies indicated their commitment to promoting greater flexibility and more efficient use of radio spectrum**. Highlights:

http://www.gao.gov/highlights/d04666high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−666

33. *May 28, General Accounting Office* — **GAO−04−321: Technology Assessment: Cybersecurity for Critical Infrastructure Protection (Report).** Computers and networks essentially run the critical infrastructures that are vital to our national defense, economic security, and public health and safety. Unfortunately, many computer systems and networks were not designed with security in mind. As a result, **the core of our critical infrastructure is riddled with vulnerabilities that could enable an attacker to disrupt operations or cause damage to these infrastructures**. Critical infrastructure protection (CIP) involves activities that enhance the security of our nation's cyber and physical infrastructure. Consistent with guidance provided by the Senate's Fiscal Year 2003 Legislative Branch Appropriations Report (S. Rpt. 107−209), GAO conducted this technology assessment in response to a request from congressional committees. **This assessment addresses the following questions: (1) What are the key cybersecurity requirements in each of the CIP sectors? (2) What cybersecurity technologies can be applied to CIP? (3) What are the implementation issues associated with using cybersecurity technologies for CIP, including policy issues such as privacy and information sharing?** Highlights: http://www.gao.gov/highlights/d04321high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−321

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: The LSASS exploit code for Windows XP has been perfected for some malicious viruses and worms, as the recent versions of the Korgo IRC Worm prove. The Watch still expects that other exploits for MS04−011 announced vulnerabilities will be perfected and used in the future.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 111 (sunrpc), 445 (microsoft−ds), 137 (netbios−ns), 1434 (ms−sql−m), 9898 (dabber), 5554 (sasser−ftp), 3127 (mydoom), 2745 (Bagle.C), 1025 (blackjack) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

34. *June 02, Voice of America* — **Saudis link dead militants to Khobar attack.** Saudi Arabia says security forces have trapped and killed two suspected militants linked to a deadly hostage−taking crisis in the eastern port city of Khobar. **An Interior Ministry statement says the hunt for suspects in the weekend's Khobar attacks led security forces to an isolated area near the western city of Taif. The statement says the suspects, one of them disguised as a woman, were trapped in an alley and killed after they began shooting at police and throwing grenades.** Twenty−two people, most of them foreigners, were killed during the 25−hour hostage ordeal in Khobar. The siege ended early Sunday, May 30, when security forces stormed a building where four gunmen were holed up with about 50 captives. Three of four suspects managed to escape.
Source: http://www.voanews.com/article.cfm?objectID=5C497FBA−480C−4BDE−9F664CFA8083B7F3

35. *June 01, CNN* — **France on red alert for D−Day.** France has gone on red security alert for the visit of a host of world leaders at the weekend for the 60th anniversary of the D−Day landings. **World leaders due to attend the commemoration include U.S. President George W. Bush, Russian President Vladimir Putin, Queen Elizabeth II of Britain along with Prime Minister Tony Blair and the monarchs of Norway and the Netherlands. Chancellor Gerhard Schroeder will also be present,** the first time a serving German leader will attend the ceremonies. Mindful of the possibility of aerial attacks, a no−fly zone is being imposed over the Normandy beaches in northern France where some 132,500 Allied troops stormed ashore on June 6, 1944. **As well as ID and baggage checks for all traveling to Normandy by train or car, public water supplies will be monitored to prevent any poisoning attempts.** Four thousand troops and an extra 1,000 police have been mobilized under the Vigipirate security plan, which will be raised to the maximum level −− scarlet −− from June 4, ahead of the arrival of dignitaries, thousands of war veterans and media.
Source: http://www.cnn.com/2004/WORLD/europe/06/01/france.dday.security/index.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer